Stottesdon and Sidbury Parish Council

Information Technology (IT) Policy

1. Purpose

This policy sets out how Stottesdon and Sidbury Parish Council uses information technology to ensure that council data is handled securely, lawfully, and effectively. It supports compliance with Assertion 10 of the Annual Governance and Accountability Return (AGAR).

2. Scope

This policy applies to:

- The Clerk
- All Councillors
- Any person who handles council information or provides technical support

It covers the use of personal or council-owned devices when used for council business.

3. Email and Communication

- The Council has approved the use of **gov.uk** email addresses.
- Councillor email addresses will follow the format:
  firstname.surname@stottesdon-pc.gov.uk
- The Clerk will use:
  clerk@stottesdon-pc.gov.uk
- Until the transition is complete, councillors using personal email accounts must:
  - keep their accounts secure with a password or PIN
  - use them solely for council business
  - store council emails in a separate folder
- Sensitive information must not be shared via unsecure platforms or forwarded to third parties.

4. Data Protection

- The Council is registered with the Information Commissioner's Office (ICO).
- All personal data must be handled in accordance with data protection legislation.
- Personal data must be stored securely and only kept for as long as necessary.
- Any Freedom of Information (FOI) or Subject Access Requests (SARs) must be referred to the Clerk immediately.

5. Devices and Security

Clerk

- The Clerk uses a secure, password-protected desktop computer dedicated to council business.

- The device is not used by others, except for occasional technical support. Anyone providing support must not access council data.
- Council documents are stored securely and backed up regularly.
- Antivirus and system updates are applied promptly.

Councillors

- Councillors may use their own laptops, tablets, or phones for council business.
- Devices must be protected with a password, PIN, fingerprint, or similar.
- Devices should be kept updated and protected with basic security measures.
- Council documents must not be stored on shared family devices.
- When a councillor leaves office, they must delete any council information they hold.

Council Laptop

- The council laptop has been wiped and is not currently used for day-to-day work.
- It may be updated and retained as a backup device if practical.

6. Home Working

- The Clerk works from home using a secure, password-protected desktop computer dedicated to council business.
- Screens must not be visible to unauthorised persons, including visitors or household members.
- Council files (electronic and paper) must be stored only in approved, secure locations such as:
    - password-protected folders
    - encrypted or secure cloud storage
    - locked drawers or cabinets for paper records
- **Paper records are locked away when not in use.**
- The home Wi-Fi network must use **WPA2 or WPA3 encryption** and be protected with a strong password.
- Public Wi-Fi must not be used for council work.
- Council documents must be backed up regularly to a secure location.
- The Clerk ensures that the home working environment protects confidentiality at all times.

7. Website Management

- The Parish Council maintains an official website at **www.stottesdon-pc.gov.uk (stottesdon-pc.gov.uk in Bing)**.
- The website is the Council's primary public information platform and must contain up-to-date statutory information, including agendas, minutes, contact details, policies, and financial documents.
- The Clerk is responsible for updating and maintaining the website, ensuring information is published promptly and accurately.
- The website will be kept accessible as far as reasonably practicable for a small authority, following government guidance on accessibility standards.
- Any technical issues or accessibility concerns will be reported to the Clerk for investigation and resolution.

8. Social Media and Community Information Sharing

- Any official council social media accounts must be clearly identified as such.
- Only authorised persons (normally the Clerk, unless the Council agrees otherwise) may post on official council accounts.
- Councillors may share or signpost official council information but must not present personal views as council policy.
- Personal social media accounts must not be used to conduct council business or discuss confidential matters.

Clerk's Use of Community Platforms

- The Clerk may share public service information (such as road closures, gritting updates, emergency notices, Police alerts, or other relevant updates from Shropshire Council or the Police) on local community platforms, including the Stottesdon Community Facebook page and local WhatsApp groups.
- These posts are provided to assist parishioners and **do not constitute official Parish Council communication**.
- No confidential or sensitive council information will be shared on these platforms.

9. Incident Reporting

- Any suspected data breach, loss of information, or IT security issue must be reported to the Clerk immediately.
- The Clerk will assess the issue and take appropriate action, including reporting to the ICO if required.

10. Training and Awareness

- The Clerk and all Councillors should receive appropriate training in:
  - **Cybersecurity**
  - **GDPR and data handling**
  - **Freedom of Information (FOI) compliance**
- Training will be proportionate to the size and needs of the Parish Council.
- The Clerk will keep up to date with relevant changes in legislation or best practice and bring any significant updates to the Council's attention.
- Refresher training will be provided when necessary.

11. Review

This policy will be reviewed annually or sooner if required due to changes in legislation, technology, or council procedures.